Executive Office
P.O. Box 942701
Sacramento, CA 94229-2701
Telecommunications Device for the Deaf - (916) 795-3240
(916) 795-3829, FAX (916) 795-3410

April 21, 2008

AGENDA ITEM 8

TO: MEMBERS OF THE FINANCE COMMITTEE

I. SUBJECT: Privacy and Security Taskforce

II. PROGRAM: Executive

III. RECOMMENDATION: Information Item

IV. ANALYSIS:

BACKGROUND

In August 2007 CalPERS mailed a brochure to retirees alerting them of the upcoming election for the retiree representative seat on the CalPERS Board of Administration, and that they would be receiving a ballot in the mail. All or part of the retired member's Social Security number was inadvertently printed above their name on the address panel of each brochure. This incident made it clear that existing internal controls needed to be reviewed, revised and strengthened to provide maximum protection of CalPERS members' personal and confidential information.

The issue of privacy and security of sensitive information has grown more complicated as the business processes upon which we heavily rely are increasingly more automated and web based. Chief Executive Officer Fred Buenrostro established an Enterprise-wide Privacy and Security Task Force to conduct a system wide review of the way we manage members' personal and confidential information, and make recommendations on steps we can take to enhance data security. The task force immediately took steps to enhance security of data. Immediate steps included: formalizing CalPERS' policies and procedures surrounding electronic file transfers. (Attachment 1)

In addition, CalPERS partnered with CSIdentity Corporation to provide credit monitoring services to members affected by a CalPERS security breach. The service includes monitoring of the individual's information via credit reports, internet site and various reports such as criminal records, names and aliases, and address history. In addition, the service includes $25,000 of identity theft

insurance as well as toll-free access to an Identity Recovery Advocate in the unlikely event that any of our members experience an identity theft event. As of April 9, 2008, 48,991 of our members took advantage of this service.. In addition to the added confidence provided members, CSIdentity indicated no breaches of security were detected.

DISCUSSION

The task force first developed an action plan that included 20 items that could be assigned and implemented quickly. To date, we have added 3 additional items and 13 of those have been completed. Approximately half of those action items have been completed. Of the remaining 10 items we believe that most, if not all, will be completed by the end of June 2008. (Attachment 2)

In order to complete an Enterprise Privacy and Security Assessment expeditiously, a consulting firm that specializes in security and privacy, Scientific Applications International Corporation (SAIC) was selected to complete an assessment of CalPERS processes, practices, policies, and procedures. SAIC has extensive experience providing government and commercial enterprises with high-level information protection and integration. It was agreed that the assessment was to include the following:

- Measurement of CalPERS processes, practices, and procedures against industry best practices and completion of a gap analysis that contrasts CalPERS against those current practices; and
- Completion of a final report and implementation plan, including both a Communication and Training Plan.

METHODOLOGY

SAIC was retained to: (1) complete a gap analysis that contrasts industry best practices with CalPERS current practices along with conclusions, (2) draft a report of findings, recommendations, and a proposed corrective action plan, and (3) a final report and implementation plan, that includes both Communication and Training Plans as an addenda to the report. In completing their work over a four month time frame, they conducted 115 interviews with staff throughout CalPERS, including a representative sample of regional offices recommended by the Member and Benefit Services Branch. They reviewed 126 separate policies, practices, and processes, and met with four organizations comparable to CalPERS with Privacy and Security Programs or processes (Caltrans, Franchise Tax Board, CalSTRS, and Department of Personnel Administration.)

The final report was received March 31, 2008. The report includes over 50 summary findings and recommendations, distributed by 11 Industry Best Practice

categories. Each recommendation was risk rated to assist us in determining what issues we should consider implementing on a scheduled basis.

The main body of the report addresses the risk and gap assessment and the resultant findings recommendations. The key findings and recommendations are divided into two major categories based on industry standards and best practices. Traditionally, security and privacy have been viewed to reside exclusively in the "technology" domain. Today, there is a growing awareness and acceptance that the major category leading to success comprises those elements within a broader category called "enterprise". The shift places emphasis and accountability at the executive level within the organization. Therefore, SAIC has structured this report and the findings and recommendations into two major categories: Enterprise Level and Technical and Operational. The first category, Enterprise Level is further broken out to six major sub-sections, strategy, governance, organization structure and design, planning and coordination, policies procedures and process, and performance management and accountability. The second category, Technical and Operations is further broken out by privacy, technical and operational sub-sections.

The final risk and gap assessment resulted in a total of fifty four (54) recommendations associated with these nine subsections. The fifty four (54) recommendations were risk rated for a total of twenty nine (29) recommendations rated as high, twenty three (23) rated as medium, and one (1) rated as low. The following factors contributed to the definition of high, medium and low risk ratings in this report, (a) what CalPERS strives to achieve vs. its current state of compliance, and the overall success of its security and privacy program based on recent breaches and security and privacy incidents, (b) actual weaknesses discovered throughout the risk and gap assessment in technology and business process and (c) the ISO's stated direction to comply with National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) 17799 standards and best practices, (d) executive management's goal of compliance to the Privacy Act, HIPAA and financial and investment laws and regulations and (d) the state of California governance within SAM and other security and privacy program guides and recommendations. The initial risk and gap assessment identified one hundred eighty (180) separate best practice control points used to assess CalPERS compliance to industry best practices, standards and legal and regulatory requirements.

The Assessment team commended CalPERS for their proactive security and privacy initiatives and the establishment of an Interim Task Force to deal with initiatives, and found that compliance with current State of California guidance and SAM has been a focus area of improvement in CalPERS, and while policies and practices are slightly out of date, the current Information Security Office

(ISOF) is in the process of updating all policies and practices that are to be complete by June 30, 2008. In addition, there are a lot of activities and projects underway to reduce risk and protect CalPERS information assets that are consistent with state guidelines and policies. However, they indicated in order for CalPERS to implement a successful Security and Privacy Program the following major recommendations should be implemented:

- Establish an enterprise wide Privacy and Security Program at the Executive level and establish a Privacy and Security Officer to manage the program;
- Consolidate responsibility and accountability for all privacy and security issues, eliminate the privacy and security fragmentation in CalPERS, and clearly define information security/privacy roles and responsibilities throughout the organization;
- Develop a long-term enterprise security and privacy strategy and an overarching enterprise security and privacy plan;
- Develop a security and privacy technology architecture and supporting documentation;
- Enhance communication and awareness;
- Enhance enforcement of security and privacy policies and practices; and
- Design an effective organizational governance structure to improve decision making and accountability.

Prior to receiving SAIC's final report, two limited term positions were established to manage the privacy and security project, provide staff support to the task force, and coordinate with CSIdentity. Also, the Office of Public Affairs has developed an extensive awareness campaign including posters, tips on the intranet, and an all staff forum concentrating on privacy and security which will be held the end of April. The focus of the efforts is to identify memorable ways employees can become security champions. A copy of the poster campaign is attached. (Attachment 3)

After a review of the findings and recommendations, the Task Force will develop the appropriate organization structure to support the implementation of a comprehensive Privacy and Security Program. Major steps include the acquisition of additional resources to develop a comprehensive, cohesive program of information security management, awareness, and accountability. This is important, not just to protect our information assets today, but will be increasingly important as CalPERS moves to a more self service orientation in business transactions through the development and implementation of the Pension System Resumption Project. Information security training for CalPERS staff will also be a key focus to ensure staff have the knowledge and resources to protect the privacy of our members.

Members of the Finance Committee
April 21, 2008

Based on the report findings, the task force has requested the following in the 2008-09 Enterprise budget:

- Establishing one new permanent position and reclassifying two positions from limited term to permanent, and

- $100,000 for additional contract services that may be needed.

V. ANALYSIS:

Under Goals III and VI of the Strategic Plan, CalPERS is committed to:

- Sustaining a high performance work culture utilizing staff development, technology, and innovative leadership and management strategies and

- Administering pension benefit services in a customer oriented and cost effective manner.

VI. RESULTS/COSTS:

Other than those mentioned above, there are no additional costs associated with this item.

_____
R.E. “Gene” REICH
Privacy and Security Taskforce
Project Consultant

_____
GLORIA MOORE ANDREWS
Deputy Executive Officer – Operations

_____
FRED BUENROSTRO
Chief Executive Officer

Attachments